



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/779,922	02/16/2004	Giovanni M. Della-Libera	MS1-1857US	8992
22801	7590	08/30/2007		
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			EXAMINER ABRISHAMKAR, KAVEH	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 08/30/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/779,922

Applicant(s)

DELLA-LIBERA ET AL.

Examiner

Kaveh Abrishamkar

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-40 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>3/5/04, 7/20/07</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in response to the communication received on February 16, 2004. Claims 1-40 was received for consideration. No preliminary amendments for the claims have been received.
2. Claims 1-40 are currently pending consideration.

Information Disclosure Statement

3. Initialed and dated copies of Applicant's IDS form 1449, received on March 5, 2004 and July 20, 2007, are attached to this Office action.

Claim Objections

4. Claim 17 is objected to because of the following informalities: There is no period at the end of the claim. A period should be placed after the word "network" in the claim. Appropriate correction is required.
5. Claim 23 is objected to because of the following informalities: There is no period at the end of the claim. A period should be placed after the word "set" in the claim. Appropriate correction is required.
6. Claims 9 and 37 are objected to because of the following informalities: The word "securitizing" is not defined in the specification, and the general definition of the term is related to finance, and unrelated to the invention. The Examiner assumes that the term

should be "securing" or an equivalent term, and the claims are rejected based upon this interpretation. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 19-29 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Independent claim 19 and the subsequent dependent claims 20-29 are deemed non-statutory because the claims are interpreted as being purely software per se. Data structures or computer programs not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See, e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760. The datastores, and the module disclosed as the components in claim 19 could be purely implemented in software, and such claimed computer programs do not define any structural and functional interrelationship between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32

Art Unit: 2131

USPQ2d at 1035. Accordingly, it is important to distinguish claims that define descriptive material per se from claims that define statutory inventions (see Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility: Annex IV).

8. Claims 13, 18, and 30-40 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The aforementioned claims disclose a "machine readable medium" that includes instructions (claims 13 and 18), or components (claims 30-40). Referring back to the specification, it is stated that combinations of either communication media, or computer storage media are within the scope of "computer readable media" (page 18, paragraph 0058), and furthermore, that communication media may be embodied in a "modulated data signal" (page 18, paragraph 0058). Therefore, the claimed "machine readable medium" can be a data signal. A signal, a form of energy, does not fall within either of the two definitions of manufacture. Thus, a signal does not fall within one of the four statutory classes of § 101 (see "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility").

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 31-40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which

Art Unit: 2131

applicant regards as the invention. The preamble of the independent claim 31 states that the claim is directed towards a "machine-readable medium," which is an article of manufacture. However, in the body of the claim, the limitations are means plus function limitations, in which the means brings in the structure of an apparatus claim. Therefore, from the structure of the claims, it is indefinite which statutory class of invention the claims are directed, and as a result, the claim is deemed indefinite.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-11, 13-15, 17, 18-27, 29-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Davis et al. (U.S. Patent 6,931,532).

Regarding claim 1, Davis discloses:

A method, comprising:

receiving a message (column 14, lines 39-54), *wherein a document (message) is received before the security policies are applied;*

selecting a first set of security information (Figure 7A, block 705, column 20, lines 38-42: *"element definition"*) from a first plurality of sets of security information (column 20, lines 45-46: *there are multiple element definitions*) as a function of a property of the message (Figure 3, column 14, lines 29-38), *wherein an element definition is define in the XML document (message)*;

selecting a second set of security information (Figure 7A, block 710, column 20, lines 45-49: *a policy object definition is retrieved*) from a second plurality of sets of security information (column 20, lines 45-57: *multiple policy objects relating to multiple element definitions*) as a function of the first set (column 20, lines 45-57), *wherein policy object is derived from the element definition*; and

applying the second set of security information to the message (Figure 7, block 715, column 21, lines 27-33), *wherein the policy object defines if encryption is necessary and the strength of encryption, and then processes the document to encrypt the necessary data elements per the associated policy.*

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Davis discloses:

The method of claim 1, wherein applying the second set of security information to the message further comprises applying security information derived from the first set (column 20, lines 45-57), *wherein policy object is derived from the element definition.*

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Davis discloses:

The method of claim 1, further comprising determining whether the message satisfies a security requirement derived from security information of the second set (column 21, lines 27-42), *wherein the policy (second set) in relation to the message to see if the message is encrypted up the correct security level.*

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Davis discloses:

The method of claim 3, wherein determining whether the message satisfies a security requirement derived from security information of the second set further comprises determining whether the message satisfies a security requirement derived from security information in the first set (column 21, lines 27-42), *wherein different policy objects (second set) are associated with different element definitions (first set) and depending on which element definition is received, the policy may require the message to be encrypted or not to be encrypted.*

Claim 5 is rejected as applied above in rejecting claim 3. Furthermore, Davis discloses:

The method of claim 3, further comprising rejecting the message if the message does not satisfy the security requirement (column 21, lines 27-42), *wherein if the message does not have the prerequisite security level, it is not passed to the client.*

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Davis discloses:

The method of claim 5, further comprising accepting the message if the message satisfies all security requirements included in the second set (column 31, lines 49-52),

wherein if the processing has been performed on the document (message), the document is delivered to a client.

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Davis discloses:

The method of claim 6, wherein the message is received after transmission from a sender (column 31, lines 49-52), *wherein if the processing has been performed on the document (message), the document is delivered to a client from the server (sender).*

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Davis discloses:

The method of claim 1, wherein the message is to be transmitted to another process (column 31, lines 49-52), *wherein if the processing has been performed on the document (message) by the server, the document is delivered to a client (another process).*

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Davis discloses:

The method of claim 8, further comprising securitizing the message before the message is transmitted (column 19, lines 58 – column 20, line 5), *wherein encryption is applied to the elements which have been tagged as needing encryption, and this application of encryption takes place during the processing phase prior to transmission of the message to a recipient.*

Art Unit: 2131

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Davis discloses:

The method of claim 1, wherein the second plurality of sets of security information are shared between nodes of a network (column 11, lines 28-33), *wherein an authorized group of clients are authorized to use a key included in the policy object (second set of security information) to decrypt the encrypted parts of the document (message), and each group includes more than one node.*

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Davis discloses:

The method of claim 1, wherein the first set is selected using an XPath-based expression to match a preselected pattern (column 12, lines 37-55), *wherein using the semantics of XML, a element definition (pattern), which has associated with it, a policy definition which is applied depending on which definition (pattern) is detected.*

Claim 13 is rejected as applied above in rejecting claim 1. Furthermore, Davis discloses:

A machine readable medium having instructions for performing the method of claim 1 (column 1, lines 18-20), *wherein the method is embodied on a computer program product.*

Regarding claim 14, Davis discloses:

A method of configuring security scheme of a node in a message-based system, the method comprising:

loading, in the node, a first plurality of sets of security information (column 20, lines 45-46: *there are multiple element definitions*) related to security requirements of an application residing in the node (Figure 7A, block 705, column 20, lines 38-42: *"element definition"*);

loading, in the node, a second plurality of sets of security information (Figure 7A, block 710, column 20, lines 45-49: *a policy object definition is retrieved*) related to another set of security requirements (column 20, lines 45-57), *wherein policy object is derived from the element definition*; and

loading, in the node, mapping information that maps a set of security information of the first plurality of sets to a set of security information of the second plurality of sets (Figure 7, block 715, column 21, lines 27-33), *wherein the element definition (first set) defines the policy object (mapped), and the policy object defines if encryption is necessary and the strength of encryption, and then processes the document to encrypt the necessary data elements per the associated policy.*

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Davis discloses:

The method of claim 13, wherein a set of the first plurality of sets can be selected using an XPath-based expression to match a preselected pattern (column 12, lines 37-55), *wherein using the semantics of XML, a element definition (pattern), which has*

Art Unit: 2131

associated with it, a policy definition which is applied depending on which definition (pattern) is detected.

Claim 17 is rejected as applied above in rejecting claim 13. Furthermore, Davis discloses:

The method of claim 13, wherein the second plurality of sets is shared between nodes of a network (column 11, lines 28-33), *wherein an authorized group of clients are authorized to use a key included in the policy object (second set of security information) to decrypt the encrypted parts of the document (message), and each group includes more than one node.*

Claim 18 is rejected as applied above in rejecting claim 14. Furthermore, Davis discloses:

A machine readable medium having instructions for performing the method of claim 14 (column 1, lines 18-20), *wherein the method is embodied on a computer program product.*

Regarding claim 19, Davis discloses:

A system comprising:

a first datastore to include a first plurality of sets of security information (column 20, lines 45-46: *there are multiple element definitions*) related to an application residing

Art Unit: 2131

in the system (column 20, lines 45-57), *wherein policy object is derived from the element definition;*

a second datastore to include a second plurality of sets of security information (Figure 7A, block 710, column 20, lines 45-49: *a policy object definition is retrieved*), wherein a set of the first plurality of sets is associated with a set of the second plurality of sets (column 20, lines 45-57), *wherein policy object is derived from the element definition;* and

a module to select a first set from the first plurality of sets as a function of a property of a received message (Figure 3, column 14, lines 29-38), *wherein an element definition is define in the XML document (message).*

Claim 20 is rejected as applied above in rejecting claim 19. Furthermore, Davis discloses:

The system of claim 19 wherein the first and second datastores are part of a single larger datastore (column 13, lines 1-7), *wherein the element definitions (first datastore) and the associated policies (second datastore) are preferably stored in a LDAP database.*

Claim 21 is rejected as applied above in rejecting claim 19. Furthermore, Davis discloses:

The system of claim 19 wherein the module is further to apply security information included in a second set of the second plurality of sets to the received

Art Unit: 2131

message (Figure 7, block 715, column 21, lines 27-33), *wherein the policy object defines if encryption is necessary and the strength of encryption, and then processes the document to encrypt the necessary data elements per the associated policy.*

Claim 22 is rejected as applied above in rejecting claim 21. Furthermore, Davis discloses:

The system of claim 21, wherein the module is further to apply security information included in the first set to the received message (Figure 7, block 715, column 21, lines 27-33), *wherein the element definition (first set) defines the policy object (mapped), and the policy object defines if encryption is necessary and the strength of encryption, and then processes the document to encrypt the necessary data elements per the associated policy.*

Claim 23 is rejected as applied above in rejecting claim 21. Furthermore, Davis discloses:

The system of claim 21, wherein the module is further to determine whether the received message satisfies a security requirement included in security information of the second set (column 21, lines 27-42), *wherein different policy objects (second set) are associated with different element definitions (first set) and depending on which element definition is received, the policy may require the message to be encrypted or not to be encrypted.*

Art Unit: 2131

Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Davis discloses:

The system of claim 23, wherein the module is further to reject the message if the message does not satisfy the security requirement (column 21, lines 27-42), *wherein if the message does not have the prerequisite security level, it is not passed to the client.*

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Davis discloses:

The system of claim 24, wherein the module is further to accept the message if the message satisfies all security requirements included in the security information of the second set (column 31, lines 49-52), *wherein if the processing has been performed on the document (message), the document is delivered to a client.*

Claim 26 is rejected as applied above in rejecting claim 19. Furthermore, Davis discloses:

The system of claim 19, further comprising a third datastore to include mappings from sets of the first plurality of sets to sets of the second plurality of sets, wherein the second set is associated with the first set by a mapping included in the third datastore (Figure 7, block 715, column 21, lines 27-33), *wherein the element definition (first set) defines the policy object (mapped), and the policy object defines if encryption is necessary and the strength of encryption, and then processes the document to encrypt*

Art Unit: 2131

the necessary data elements per the associated policy.

Claim 27 is rejected as applied above in rejecting claim 19. Furthermore, Davis discloses:

The system of claim 19, wherein the module is to select the first set using an XPath-based expression to match a preselected pattern (column 12, lines 37-55), *wherein using the semantics of XML, a element definition (pattern), which has associated with it, a policy definition which is applied depending on which definition (pattern) is detected.*

Claim 28 is rejected as applied above in rejecting claim 19. Furthermore, Davis discloses:

The system of claim 19, wherein the second plurality of sets are shared between nodes of the system (column 11, lines 28-33), *wherein an authorized group of clients are authorized to use a key included in the policy object (second set of security information) to decrypt the encrypted parts of the document (message), and each group includes more than one node.*

Claim 30 is rejected as applied above in rejecting claim 19. Furthermore, Davis discloses:

A machine readable medium having components as recited in claim 19 (column 1, lines 18-20), *wherein the method is embodied on a computer program product.*

Regarding claim 31, Davis discloses:

A machine-readable medium having components, comprising:

means for receiving a message (column 14, lines 39-54), *wherein a document (message) is received before the security policies are applied;*

means for selecting a first set of security information (Figure 7A, block 705, column 20, lines 38-42: *"element definition"*) from a first plurality of sets of security information (column 20, lines 45-46: *there are multiple element definitions*) as a function of a property of the message (Figure 3, column 14, lines 29-38), *wherein an element definition is define in the XML document (message);*

means for selecting a second set of security information (Figure 7A, block 710, column 20, lines 45-49: *a policy object definition is retrieved*) from a second plurality of sets of security information (column 20, lines 45-57: *multiple policy objects relating to multiple element definitions*) as a function of the first set (column 20, lines 45-57), *wherein policy object is derived from the element definition; and*

means for applying the second set of security information to the message (Figure 7, block 715, column 21, lines 27-33), *wherein the policy object defines if encryption is necessary and the strength of encryption, and then processes the document to encrypt the necessary data elements per the associated policy.*

Claim 32 is rejected as applied above in rejecting claim 31. Furthermore, Davis discloses:

The machine-readable medium of claim 31, further comprising means for determining whether the message satisfies a security requirement derived from the first and/or second sets (column 21, lines 27-42), *wherein different policy objects (second set) are associated with different element definitions (first set) and depending on which element definition is received, the policy may require the message to be encrypted or not to be encrypted.*

Claim 33 is rejected as applied above in rejecting claim 32. Furthermore, Davis discloses:

The machine-readable medium of claim 32, further comprising means for rejecting the message if the message does not satisfy the security requirement (column 21, lines 27-42), *wherein if the message does not have the prerequisite security level, it is not passed to the client.*

Claim 34 is rejected as applied above in rejecting claim 32. Furthermore, Davis discloses:

The machine-readable medium of claim 32, further comprising means for accepting the message if the message satisfies all security requirements derived from the first and second sets (column 31, lines 49-52), *wherein if the processing has been performed on the document (message), the document is delivered to a client.*

Art Unit: 2131

Claim 35 is rejected as applied above in rejecting claim 34. Furthermore, Davis discloses:

The machine-readable medium of claim 34, wherein the message is received after transmission from a sender (column 31, lines 49-52), *wherein if the processing has been performed on the document (message), the document is delivered to a client from the server (sender).*

Claim 36 is rejected as applied above in rejecting claim 31. Furthermore, Davis discloses:

The machine-readable medium of claim 31, wherein the message is to be transmitted to another process (column 31, lines 49-52), *wherein if the processing has been performed on the document (message) by the server, the document is delivered to a client (another process).*

Claim 37 is rejected as applied above in rejecting claim 36. Furthermore, Davis discloses:

The machine-readable medium of claim 36, further comprising means for securitizing the message before the message is transmitted (column 19, lines 58 – column 20, line 5), *wherein encryption is applied to the elements which have been tagged as needing encryption, and this application of encryption takes place during the processing phase prior to transmission of the message to a recipient.*

Art Unit: 2131

Claim 38 is rejected as applied above in rejecting claim 31. Furthermore, Davis discloses:

The machine-readable medium of claim 31, wherein the second plurality of sets of security information are shared between nodes of a network (column 11, lines 28-33), *wherein an authorized group of clients are authorized to use a key included in the policy object (second set of security information) to decrypt the encrypted parts of the document (message), and each group includes more than one node.*

Claim 39 is rejected as applied above in rejecting claim 31. Furthermore, Davis discloses:

The machine-readable medium of claim 31, wherein the means for selecting the first set uses an XPath-based expression to match a preselected pattern (column 12, lines 37-55), *wherein using the semantics of XML, a element definition (pattern), which has associated with it, a policy definition which is applied depending on which definition(pattern) is detected.*

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2131

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 12, 16, 28, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (U.S. Patent 6,931,532) in view of Hartman et al. (U.S. Patent 6,807,636).

Claim 12 is rejected as applied above in rejecting claim 1. Davis does not explicitly state that the first set is selected using Simple Object Access Protocol (SOAP) actions. Hartman discloses a system for facilitating security in a network which is used to facilitate security requests which can be associated for a specific environment including document exchange frameworks including SOAP and XML (column 32, lines 35-46). Hartman discloses receiving a security request and processing the request, independent of which document exchange framework is used (column 32, lines 33-36). Davis and Hartman are analogous arts as both provide security in a document exchange framework environment. Processing SOAP messages, as is done in Hartman, in the system of Davis, would allow the system to support security for both kinds of document requests. It is well-known that SOAP messages, include an envelope with a header and a body. The element definition information, as taught by Davis, which is in the XPath information in XML, could be placed in the header or the body of the envelope for the parser to recognize, and allows a policy to be associated with the element definition. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the SOAP message capability of Hartman in the system of Davis "to provide methods and apparatus that facilitated integrated security across the perimeter, middle, and back-office security tiers while allowing the

Art Unit: 2131

use of applications and security services that are from different vendors and/or that are based or operating on different platforms” (Hartman: column 2, lines 35-39).

Claim 16 is rejected as applied above in rejecting claim 13. Davis does not explicitly state that the first set is selected using Simple Object Access Protocol (SOAP) actions.

Hartman discloses a system for facilitating security in a network which is used to facilitate security requests which can be associated for a specific environment including document exchange frameworks including SOAP and XML (column 32, lines 35-46).

Hartman discloses receiving a security request and processing the request, independent of which document exchange framework is used (column 32, lines 33-36).

Davis and Hartman are analogous arts as both provide security in a document exchange framework environment. Processing SOAP messages, as is done in Hartman, in the system of Davis, would allow the system to support security for both kinds of document requests. It is well-known that SOAP messages, include an envelope with a header and a body. The element definition information, as taught by Davis, which is in the XPath information in XML, could be placed in the header or the body of the envelope for the parser to recognize, and allows a policy to be associated with the element definition. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the SOAP message capability of Hartman in the system of Davis “to provide methods and apparatus that facilitated integrated security across the perimeter, middle, and back-office security tiers while allowing the

Art Unit: 2131

use of applications and security services that are from different vendors and/or that are based or operating on different platforms” (Hartman: column 2, lines 35-39).

Claim 28 is rejected as applied above in rejecting claim 19. Davis does not explicitly state that the first set is selected using Simple Object Access Protocol (SOAP) actions.

Hartman discloses a system for facilitating security in a network which is used to facilitate security requests which can be associated for a specific environment including document exchange frameworks including SOAP and XML (column 32, lines 35-46).

Hartman discloses receiving a security request and processing the request, independent of which document exchange framework is used (column 32, lines 33-36).

Davis and Hartman are analogous arts as both provide security in a document exchange framework environment. Processing SOAP messages, as is done in Hartman, in the system of Davis, would allow the system to support security for both kinds of document requests. It is well-known that SOAP messages, include an envelope with a header and a body. The element definition information, as taught by Davis, which is in the XPath information in XML, could be placed in the header or the body of the envelope for the parser to recognize, and allows a policy to be associated with the element definition. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the SOAP message capability of Hartman in the system of Davis “to provide methods and apparatus that facilitated integrated security across the perimeter, middle, and back-office security tiers while allowing the

Art Unit: 2131

use of applications and security services that are from different vendors and/or that are based or operating on different platforms" (Hartman: column 2, lines 35-39).

Claim 40 is rejected as applied above in rejecting claim 31. Davis does not explicitly state that the first set is selected using Simple Object Access Protocol (SOAP) actions.

Hartman discloses a system for facilitating security in a network which is used to facilitate security requests which can be associated for a specific environment including document exchange frameworks including SOAP and XML (column 32, lines 35-46).

Hartman discloses receiving a security request and processing the request, independent of which document exchange framework is used (column 32, lines 33-36).

Davis and Hartman are analogous arts as both provide security in a document exchange framework environment. Processing SOAP messages, as is done in Hartman, in the system of Davis, would allow the system to support security for both kinds of document requests. It is well-known that SOAP messages, include an envelope with a header and a body. The element definition information, as taught by Davis, which is in the XPath information in XML, could be placed in the header or the body of the envelope for the parser to recognize, and allows a policy to be associated with the element definition. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the SOAP message capability of Hartman in the system of Davis "to provide methods and apparatus that facilitated integrated security across the perimeter, middle, and back-office security tiers while allowing the

Art Unit: 2131

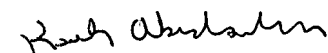
use of applications and security services that are from different vendors and/or that are based or operating on different platforms" (Hartman: column 2, lines 35-39).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000


Kaveh Abrishamkar 8/29/07
AU 2131

K.A.
KA
08/28/2007